ABSTRACT

One aspect of the present invention establishes a session key by a receiving unit R transmitting a plurality of quantities for storage in a public repository. A sending unit S:

1. retrieves the plurality of quantities; and
2. computes and transmits to the unit R a plurality of sender's quantities; and
3. using at least one of the plurality of public quantities, computes the session key K.

The unit R, using the sender's quantities:

1. computes and transmits to the unit S at least one receiver's quantity; and
2. computes the session key.

Another aspect provides a digital signature. Before transmitting a signed message, the unit S stores a plurality of quantities in the public repository. A unit R, that receives the message and the digital signature, verifies their authenticity by:

1. retrieving the quantities from the repository;
2. using the digital signature and the quantities, evaluates expressions in at least two (2) different relationships; and
3. verifies the digital signature upon finding equality between evaluation results.